DETAILED ACTION

1. Claims 1-3 are pending.

Response to Arguments

2. Applicant's arguments filed 1/24/2010 have been fully considered but they are not persuasive.

Claim 1 is currently amended to further include the inverse of the secret information. The inverse of the secret information is not defined nor particularly recited to what constitutes an inverse of the secret information. Hence, can broadly and reasonably be interpreted as decryption data/information to the secret information such as decryption key, public key, or even another secret data that is the inverse form of data able to decrypt the secret information. Gilbert discusses symmetrical where two entities share exactly the same information (i.e. secret key) and asymmetrical where one or the two entities has a pair of keys one of which is a secret and the other is a public (col.1, lines 32-37). This reads onto the claimed secret information and the inverse of the secret information both the symmetrical and asymmetrical cryptography discloses two keys where one of the two is the inverse of the other. As for Matumoto also includes decipher means for deciphering the received cipher text to plain text using the shared key k (col.4, lines 1-15). Therefore, both references read on the claimed the inverse of the secret information.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-3 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gilbert, et al. (US 7,165,177), and further in view of Matumoto, et al. (US 5,0167,276).

As per claim 1:

Gilbert discloses a plurality of integrated circuits, each of the integrated circuits **(col.1, lines 13-14 and col.4, lines 14-15)** comprising a processor and flash memory **(col.5, lines 39-40 and col.7, lines 41-53)**, and including code for running identical software processes, wherein each of the integrated circuits also includes secret information used by the software process **(col.2, lines 4-10 and col.6, lines 11-14; secret information can broadly interpret as data that is protected and secure such that may involve authentication or verification process. Gilbert's secret key, authentication data, or certificate value (col.3, lines 1-28) which is referring to the claimed secret information.)** and the inverse of the secret information, the secret information and the inverse of the secret information **(col.1, lines 33-40 and col.3, lines 1-39; 1st and 2nd keys)** in each chip being located in a different location in the flash memory relative to locations in which *the same secret information and the inverse of the secret information is stored in the flash memory of a plurality of the other chips.* **(col.6, lines 18-22 and col.7, lines 55-65)**

The claimed inverse of the secret information can broadly be interpreted as decryption data/information to the secret information such as decryption key, public key, or even another secret data that is the inverse form of data able to decrypt the secret information. Gilbert discusses symmetrical where two entities share exactly the same information (i.e. secret key) and asymmetrical where one or the two entities has a pair of keys one of which is a secret and the other is a public (col.1, lines 32-37). This reads onto the claimed secret information and the inverse of the secret information both the symmetrical and asymmetrical cryptography discloses two keys where one of the two is the inverse of the other. Gilbert discloses the invention that provides hardwired logic or microprocessor integrated circuit chips with protection against fraud (col.1, lines 10-15). Gilbert discusses passing directly over each bit of the non-volatile memory by the number of bits determines to prevent any attempt at fraudulent replaying and the number of m is the same as the number of bits in the certificate S where the masked certificate S does not reveal any information on the certificate (col.6, lines 18-67 and col.7, lines 1-25). Gilbert teaches an EEPROM which is a type of nonvolatile memory and that a flash memory is also a type of nonvolatile memory. Although, Gilbert discloses the secret information in each chip being located in a different location in the EEPROM (flash) memory, but did not go into details in which the same secret information and the inverse of the secret information is stored in the flash memory of a plurality of the other chips.

Matumoto discloses a shared cryptokey generation system provided with a secret algorithm generation apparatus which, under requirements determined among a

plurality of entities sharing a cryptokey (col.2, lines 42-46 and col.4, lines 23-27). The plurality of entities and a plurality of cryptokey generation means are memories which store at least the secret algorithms (col.2, lines 52-55 and col.4, lines 43-55). Matumoto discloses the procedure for generating the shared cryptokeys may be performed internally in the IC cards, etc., (col.9, lines 28-65) in addition to being performed by simply inputting the identifiers, so the burden of work of the entities for sharing the cryptokeys is cut down tremendously (col.5, lines 58-63). Matumoto also includes decipher means for deciphering the received cipher text to plain text using the shared key k (col.4, lines 1-15).

Therefore, it would have been obvious for a person of ordinary skills in the art to at the time the invention was made to combine Gilbert and Matumoto to teach the same secret information and the inverse of the secret information is stored in the flash memory of a plurality of the other chips because the burden of work of the entities for sharing the cryptokeys is cut down tremendously (Matumoto - col.2, lines 42-46 and col.4, lines 5-27 and col.5, lines 58-63).

As per claim 2: see Gilbert on col.6, lines 18-22 and col.7, lines 55-65; discussing a plurality of integrated circuits according to claim 1, wherein the code on each integrated circuit is such that the software process of each chip knows the location in memory via which the secret information is accessible.

As per claim 3: a method of manufacturing a plurality of the integrated circuits of claim 2, including the steps of: manufacturing a plurality of physical integrated circuits; and (Gilbert-col.5, lines 21-23) injecting, into the flash memory of each of the integrated

circuits: code for running a software process; and the same secret information (Matumoto - col.5, lines 58-63); wherein the secret information is positioned in relatively different locations of the flash memories of the integrated circuits and the code on each integrated circuit is such that the software process of each integrated circuit knows the location in memory via which the secret information is accessible on that integrated circuit. (Gilbert-col.6, lines 18-22 and col.7, lines 55-65)

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Leynna T. Truvan whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/L. T. T./
Examiner, Art Unit 2435

/Kimyen Vu/
Supervisory Patent Examiner, Art Unit 2435